PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-122931
(43)Date of publication of application : 28.04.2000

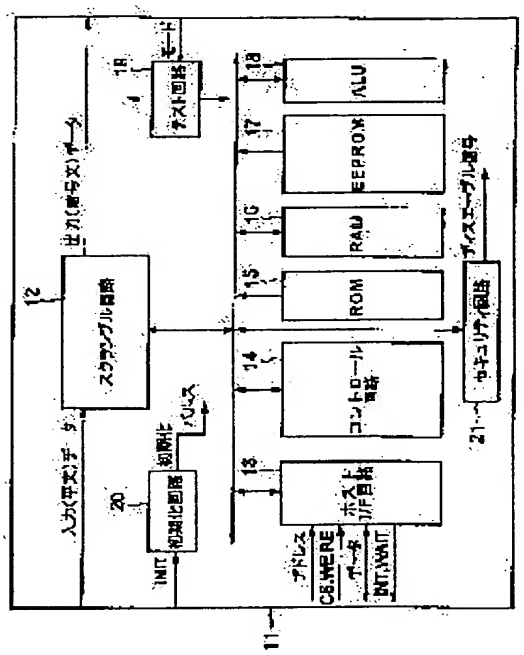
(51)Int.Cl. G06F 12/14
G06F 9/06
H04L 9/10

(21)Application number : 10-293715
(22)Date of filing : 15.10.1998

(71)Applicant : TOSHIBA CORP
(72)Inventor : MOTAI MASAHIKO

(54) DIGITAL INTEGRATED CIRCUIT

(57)Abstract:
PROBLEM TO BE SOLVED: To securely stop secret data from being accessed from outside and to easily perform reliable inspection at the time of a test by providing a control means which disables the external access to a specific storage area when specific data are written from outside.
SOLUTION: A ROM 15 stores fixed data such as open key data and programs. A RAM 16 provides an I/F area and a computing operation area for data communication with an external computer. Further, an EEPROM 17 functions to rewrite data different for every device and store data without a battery. Then a security circuit 21 as a control means performs control when certain specific data are inputted so that the area where secret data of each circuit part are written can not be accessed from outside. Before the specific data are inputted, respective circuit parts can freely be accessed from outside and a test can easily be conducted.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－122931
（P2000－122931A）
(43)公開日　平成12年４月28日(2000.4.28)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ａ	５Ｂ０１７
9/06	５５０	9/06	５５０Ｚ	５Ｂ０７６
Ｈ０４Ｌ　9/10		Ｈ０４Ｌ　9/00	６２１Ａ	５Ｊ１０４

審査請求　未請求　請求項の数10　ＯＬ　（全 11 頁）

(21)出願番号　特願平10－293715

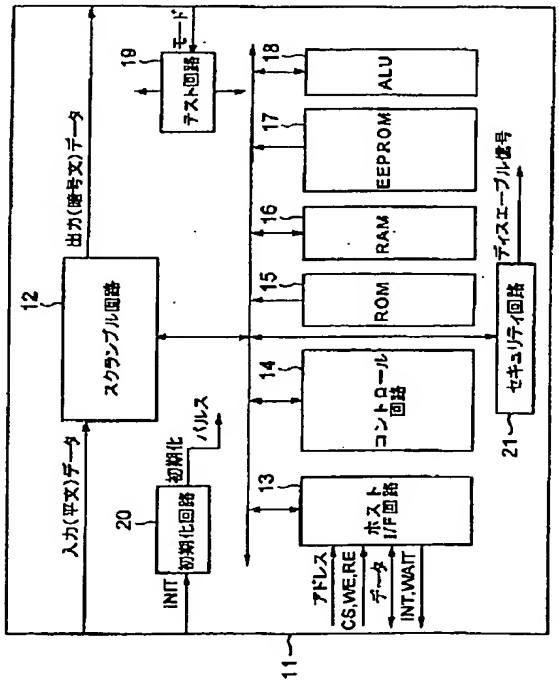
(22)出願日　平成10年10月15日(1998.10.15)

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　馬渡　正彦
神奈川県川崎市幸区柳町70番地　株式会社東芝柳町工場内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

Ｆターム(参考)　5B017 AA01 BA01 BA07 BB03 CA12
5B076 AB10 CA08 FA02 FA14
5J104 AA01 AA16 EA08 NA27 NA39
NA43

(54)【発明の名称】　デジタル集積回路

(57)【要約】
【課題】この発明は、秘匿データに対しては外部からのアクセスを確実に阻止することができ、テスト時には信頼性の高い検査を容易に行ない得るようにしたデジタル集積回路を提供することを目的としている。
【解決手段】外部からのアクセスが可能で、内部に秘匿すべきデータが書き込まれる特定記憶領域を含む記憶手段１５，１６，１７を備えたデジタル集積回路において、外部から特定データが書き込まれることにより、特定記憶領域への外部からのアクセスを不可とする制御手段２１を備えている。



【特許請求の範囲】

【請求項１】　外部からのアクセスが可能で、内部に秘匿すべきデータが書き込まれる特定記憶領域を含む記憶手段を備えたデジタル集積回路において、
外部から特定データが書き込まれることにより、前記特定記憶領域への外部からのアクセスを不可とする制御手段を具備してなることを特徴とするデジタル集積回路。

【請求項２】　前記制御手段は、前記特定データが書き込まれた状態で、その制御出力を外部から変更不能となることを特徴とする請求項１記載のデジタル集積回路。

【請求項３】　前記制御手段は、前記特定データが書き込まれた状態で、その特定データの書き替えが不可となることを特徴とする請求項１記載のデジタル集積回路。

【請求項４】　前記制御手段は、前記特定データが書き込まれた状態で、その特定データの書き替えが不可となるとともに、その制御出力を外部から変更不能となることを特徴とする請求項１記載のデジタル集積回路。

【請求項５】　前記制御手段は、
外部からデータが書き込まれるもので、データの書き込みが１回だけ可能なワンタイムメモリと、
予め設定された固定データが記憶された記憶部と、
この記憶部の固定データと前記ワンタイムメモリの内容とが一致した状態で、前記記憶手段の特定記憶領域への外部からのアクセスを不可とするための出力を発生する制御部とを具備してなることを特徴とする請求項１記載のデジタル集積回路。

【請求項６】　前記制御手段は、
外部からデータが書き込まれるメモリと、
予め設定された固定データが記憶された記憶部と、
この記憶部の固定データと前記メモリの内容とが一致した状態で、前記記憶手段の特定記憶領域への外部からのアクセスを不可とするための出力を発生するとともに、前記メモリに対する外部からのデータ書き込み及びデータ読み出しを不可とする制御部とを具備してなることを特徴とする請求項１記載のデジタル集積回路。

【請求項７】　前記制御部は、前記記憶手段の特定記憶領域への外部からのアクセスを不可とするための出力に基づいて、前記メモリの書き込みイネーブル端を書き込み不能状態に設定するとともに、前記メモリから読み出しデータを外部に出力することを制限するゲート手段を遮断状態に設定することを特徴とする請求項６記載のデジタル集積回路。

【請求項８】　前記制御手段は、
外部から初期化が要求された状態で、前記記憶手段の特定記憶領域のアドレスを指定する指定手段と、
この指定手段で指定されたアドレスに記憶された内容が書き込まれる第１の記憶部と、
予め設定された固定データが記憶された第２の記憶部と、
この第２の記憶部に記憶された固定データと前記第１の記憶部の内容とが一致した状態で、前記記憶手段の特定記憶領域への外部からのアクセスを不可とするための出力を発生する制御部とを具備してなることを特徴とする請求項１記載のデジタル集積回路。

【請求項９】　前記制御部は、前記記憶手段の特定記憶領域への外部からのアクセスを不可とするための出力が発生された状態で、前記記憶手段の記憶領域を、データの書き込み及び読み出しが共に可能な領域と、データの読み出しのみが可能な領域と、外部からのアクセスが不可な前記特定記憶領域とに分けることを特徴とする請求項８記載のデジタル集積回路。

【請求項１０】　前記記憶手段及び前記制御手段は、パッケージ内に封止されていることを特徴とする請求項１記載のデジタル集積回路。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、秘匿すべきデジタルデータを外部からアクセス不可能に保護するデジタル集積回路の改良に関する。

【０００２】

【従来の技術】周知のように、例えばデジタルデータに暗号化処理を施すためのデジタル集積回路にあっては、暗号化処理の鍵となるデータや、その暗号化処理アルゴリズムを実行するためのプログラムデータ等のような秘匿すべきデータが、内部メモリに記憶されることになる。

【０００３】この場合、デジタル集積回路には、その内部メモリ内に記憶された秘匿データが、外部から不正に読み出されたり書き替えられたりすることのないように、つまり、秘匿データを外部からアクセスすることが不可能になるように、保護対策が講じられている。

【０００４】一方、この種のデジタル集積回路においては、工場で製造された後、その内部メモリを含む各種の内部回路が正常に動作するか否かを確かめるためのテストが行なわれる。このテストとしては、実際に各種の内部回路に所定のデータを入力して、期待した出力が得られる否かを確認する手法がとられている。

【０００５】このため、上記したように、内部メモリに対して、そこに記憶されたデータを外部からアクセス不可能となるように保護対策が施されているという点と、製造時のテストを容易に行なえるようにする点とは、相反する技術となり、このことが、デジタル集積回路の設計製造を困難なものとしている。

【０００６】通常、ＬＳＩ（Large Scale Integrated circuit）製造時の検査は、ＬＳＩテスターを用いて行なわれており、短時間で済ませることができ、しかも検査されていない回路部分を極力少なくすることが要求されている。特に、ＬＳＩ内部のＲＡＭ（Random Access Memory）の検査では、その全アドレスに渡って書き込みと読み出しとが正常に行なわれるか否かを調べる必要があ

る。

【０００７】このためには、ＬＳＩの各回路部分毎にそれぞれテストモードを設定し、例えばＲＡＭのテストモードを指定すると、ＲＡＭのアドレス端子とデータ端子とがＬＳＩの接続ピンを介してテスターと接続され、また、暗号化処理のための特殊演算回路のテストモードを指定すると、その回路の入出力端子がＬＳＩの接続ピンを介してテスターと接続されるように、ＬＳＩを設計している。

【０００８】一方、外部からアクセス不可能となるように保護対策が施される回路部分については、ＬＳＩ内部の素子を接続するワイヤーを電源端や接地端に接続して固定データを作り、公開された暗号の手続に沿ってのみテストを行なうことが可能になっている。また、検査途中のデータが外部に漏れないように、各回路部分の出力が外部に出ないように考慮されている。

【０００９】このように、中間データをＬＳＩ外部に取り出すことができず、公開された暗号の手続に沿ってのみしかテストすることができないとなると、特定の回路を検査するのに複数の回路を経由しての検査となるため、テストのための入力データパターンが長くなるとともに、被検査部分の回路素子をできるだけ多く活性化させるということも困難になる。

【００１０】特に、秘匿データが、１つ１つのＬＳＩ毎、あるいはそのＬＳＩを搭載した１つ１つの機器毎に異なる場合には、例えば特開平７－４５７８２号公報に示されるように、ＬＳＩ毎あるいは機器毎に異なるデータを書き込み及び読み出しするためのデータチップと、暗号化処理するためのチップとを同一の基板上にモールドする等の処理が必要になってくる。

【００１１】ここで、従来では、例えば特開平５－７５５９７号公報等に示されるような、暗号処理ＬＳＩＣが提案されている。この暗号処理ＬＳＩＣは、秘匿データを記憶するメモリ部と、このメモリ部から読み出されるデータの外部への出力可否を制御する制御部と、メモリ部への秘匿データの書き込みアドレスを記憶する記憶部と、この記憶部に記憶された書き込みアドレスとメモリ部への読み出しアドレスとを比較する比較部とを備え、テストモードでかつ比較部の比較結果が一致した場合にのみ、制御部を出力可に制御するようにしたものである。

【００１２】しかしながら、この暗号処理ＬＳＩＣでは、テストモードに設定されたとき、記憶部の全記憶内容がリセットされることが必要条件となる。このため、実際の使用状態において、何らかの原因でテストモードに投入されてしまうと、再度、メモリ部に秘匿データを書き込み、その書き込みアドレスを記憶部に記憶させるという作業が必要になるので、使用者にとって取り扱いが不便になるという問題が生じている。

【００１３】【発明が解決しようとする課題】以上のように、従来のデジタル集積回路では、秘匿データを外部からアクセス不可能となるように保護する点と、製造時のテストを容易に行なえるようにする点とが、それぞれ十分実用に供し得るレベルにまで達していないという問題を有している。

【００１４】そこで、この発明は上記事情を考慮してなされたもので、秘匿データに対しては外部からのアクセスを確実に阻止することができ、テスト時には信頼性の高い検査を容易に行ない得るようにした極めて良好なデジタル集積回路を提供することを目的とする。

【００１５】【課題を解決するための手段】この発明に係るデジタル集積回路は、外部からのアクセスが可能で、内部に秘匿すべきデータが書き込まれる特定記憶領域を含む記憶手段を備えたものを対象としている。そして、外部から特定データが書き込まれることにより、特定記憶領域への外部からのアクセスを不可とする制御手段を備えるようにしたものである。

【００１６】上記のような構成によれば、外部から特定データが書き込まれる前は、記憶手段に対して特定記憶領域も含めて外部からアクセス可能であるため、信頼性の高いテストを容易に行なうことができる。また、外部から特定データが書き込まれた後は、記憶手段の特定記憶領域が外部からアクセス不可となるので、秘匿データに対しては外部からのアクセスを確実に阻止することができる。

【００１７】【発明の実施の形態】以下、この発明の実施の形態について図面を参照して詳細に説明する。まず、図７は、この実施の形態で説明するデジタルＬＳＩチップ１０の外観を示している。このデジタルＬＳＩチップ１０は、以下に述べる各種の回路が形成された半導体基板１１を樹脂製パッケージ内に封止してなる本体１０ａと、この本体１０ａから突出する複数のリード１０ｂとから構成されている。

【００１８】図１は、上記半導体基板１１に形成された各種の回路を示している。まず、スクランブル回路１２は、入力された平文データにスクランブル処理を施し、暗号文データに変換して出力している。

【００１９】また、ホストＩ／Ｆ（Inter/Face）回路１３は、デジタルＬＳＩチップ１０の外部に設けられた図示しないコンピュータと通信を行なうためのインターフェースである。このホストＩ／Ｆ回路１３は、コンピュータから送出されるアドレスデータ，チップセレクト信号ＣＳ，書き込みイネーブル信号ＷＥ及び読み出しイネーブル信号ＲＥ等を入力する機能と、データをコンピュータと双方向通信する機能と、割り込み信号ＩＮＴ及び待機信号ＷＡＩＴ等をコンピュータに出力する機能とを有している。

【００２０】コントロール回路１４は、デジタルＬＳＩチップ１０内部の制御や、暗号鍵解凍プログラムの演算制御を行なっている。ＲＯＭ（Read Only Memory）１５は、公開鍵データやプログラム等の固定データを記憶している。ＲＡＭ１６は、外部コンピュータとのデータ通信を行なう際のＩ／Ｆエリアや、計算作業エリアを提供している。

【００２１】さらに、ＥＥＰ（Electrically Erasable and Programmable）ＲＯＭ１７は、機器毎に異なるデータを書き替え可能で、電池がなくてもデータを保存する機能を有している。ＡＬＵ（Arithmetic Logical Unit）１８は、暗号化のための特殊演算を行なう特別の四則演算器である。

【００２２】また、テスト回路１９は、外部入力されるテストモード信号に基づいて、各回路部分を選択的にデジタルＬＳＩチップ１０の外部から検査し得る状態に切り替える。初期化回路２０は、機器の電源投入時に供給される初期化要求信号ＩＮＩＴに基づいて、各回路部分を初期化するための初期化パルスを発生する。

【００２３】ここで、セキュリティ回路２１は、詳細は後述するが、ある特定のデータが入力されると、各回路部分の秘匿データが書き込まれている領域を外部からアクセスすることができないように制御する。また、特定のデータが入力される前は、各回路部分が自由に外部からアクセスでき、テストを容易に行なえるようになっている。

【００２４】図２は、上記ホストＩ／Ｆ回路１３及びセキュリティ回路２１の詳細な構成を示している。すなわち、ホストＩ／Ｆ回路１３から出力される書き込みデータＷＤＡＴＡは、セキュリティ回路２１のワンタイムＲＯＭ２２の書き込みデータ入力端に供給されている。

【００２５】このワンタイムＲＯＭ２２は、１度だけのデータの書き込みを可能とする不揮発性メモリである。このワンタイムＲＯＭ２２の読み出しデータ出力端は、そのビット毎に設けられた複数（図では簡単のため１個のみ示す）のＥＸ（exclusive）オア回路２３の一方の入力端に接続されている。

【００２６】これらＥＸオア回路２３の他方の入力端には、不揮発性のメモリ２４に記憶された固定データが供給されている。これらＥＸオア回路２３の各出力は、オア回路２５によって論理和演算処理された後、フリップフロップ回路２６にラッチされる。

【００２７】すなわち、このＥＸオア回路２３，オア回路２４及びフリップフロップ回路２６は、ワンタイムＲＯＭ２２に書き込まれたデータと、メモリ２４に記憶された固定データとの一致を判別している。そして、両データが一致している場合に、Ｌ（Low）レベルのディスエーブル信号が、セキュリティ回路２１の出力として各回路部分に供給される。

【００２８】また、このディスエーブル信号は、アンド回路２７に供給されて、ホストＩ／Ｆ回路１３から出力される書き込みイネーブル信号ＷＥと、ホストＩ／Ｆ回路１３のアドレスデコーダ２８から出力される第４のチップセレクト信号ＣＳ４と、論理積演算される。このアンド回路２７の出力が、ワンタイムＲＯＭ２２の書き込みイネーブル端に供給されている。

【００２９】図２に示す構成において、まず、デジタルＬＳＩチップ１０の製造後の検査時には、ワンタイムＲＯＭ２２には何もデータが書き込まれておらず、メモリ２４の固定データとの一致がとられていないため、セキュリティ回路２１からは、Ｈ（High）レベルのディスエーブル信号が出力されている。

【００３０】この状態では、外部から各回路部分が自由にアクセスでき、容易にテストを行なうことができる。ただし、ワンタイムＲＯＭ２２は、一旦データを書き込んでしまうと書き替えができないため、その書き込み読み出しテストは行なわないようになされている。

【００３１】テストが終了した後、その検査用のテスターで直接に、または、外部コンピュータからホストＩ／Ｆ回路１３を介して、ワンタイムＲＯＭ２２に、メモリ２４に記憶されている固定データと同じ値の特定データを書き込む。すると、ワンタイムＲＯＭ２２に書き込まれたデータと、メモリ２４の固定データとが一致するので、セキュリティ回路２１からは、Ｌレベルのディスエーブル信号が出力される。

【００３２】この状態では、デジタルＬＳＩチップ１０の各回路部分のうち、秘匿データが書き込まれている部分が外部からアクセスできないように設定される。そして、このようにワンタイムＲＯＭ２２に、メモリ２４に記憶されている固定データと同じ値の特定データが書き込まれると、ワンタイムＲＯＭ２２の内容は書き替えることができないため、以後、ディスエーブル信号はＬレベルに固定され、秘匿データが確実に保護されることになる。

【００３３】図３は、上記したディスエーブル信号を発生するための他の例を示している。すなわち、セキュリティ回路２１には、ワンタイムＲＯＭ２２に代えてＥＥＰＲＯＭ２９が設置されている。そして、ホストＩ／Ｆ回路１３から出力される書き込みデータＷＤＡＴＡが、ＥＥＰＲＯＭ２９の書き込みデータ入力端に供給されている。

【００３４】また、上記フリップフロップ回路２６から出力されるディスエーブル信号と、ホストＩ／Ｆ回路１３から出力される書き込みイネーブル信号ＷＥと、ホストＩ／Ｆ回路１３のアドレスデコーダ２８から出力される第４のチップセレクト信号ＣＳ４とを論理積演算するアンド回路２７の出力が、ＥＥＰＲＯＭ２９の書き込みイネーブル端に供給されている。

【００３５】さらに、ＥＥＰＲＯＭ２９の読み出しデータ出力端は、上記ＥＸオア回路２３の一方の入力端に接

続されるとともに、３ステートバッファ３０を介して、読み出しデータＲＤＡＴＡの伝送ラインに接続されている。

【００３６】そして、フリップフロップ回路２６から出力されるディスエーブル信号と、ホストＩ／Ｆ回路１３から出力される読み出しイネーブル信号ＲＥと、ホストＩ／Ｆ回路１３のアドレスデコーダ２８から出力される第４のチップセレクト信号ＣＳ４とを論理積演算するアンド回路３１の出力が、３ステートバッファ３０のイネーブル端に供給されている。

【００３７】図３に示す構成において、外部コンピュータによってセキュリティ回路２１のＥＥＰＲＯＭ２９に、メモリ２４に記憶されている固定データと同じ値の特定データを書き込む。すると、ＥＥＰＲＯＭ２９に書き込まれたデータと、メモリ２４の固定データとが一致するので、セキュリティ回路２１からは、Ｌレベルのディスエーブル信号が出力される。

【００３８】このようにして、ディスエーブル信号が一旦Ｌレベルになると、アンド回路２７の出力、つまり、ＥＥＰＲＯＭ２９の書き込みイネーブル端がＬレベルになるので、以後、ＥＥＰＲＯＭ２９に対するデータの書き替えは行なわれないようになる。

【００３９】また、ディスエーブル信号が一旦Ｌレベルになると、アンド回路３１の出力、つまり、３ステートバッファ３０のイネーブル端がＬレベルになるので、以後、ＥＥＰＲＯＭ２９から読み出された特定データが読み出しデータＲＤＡＴＡの伝送ラインに供給されないようになり、特定データが外部に読み出されることが防止されるようになる。

【００４０】一方、デジタルＬＳＩチップ１０の製造直後のテスト時には、ＥＥＰＲＯＭ２９には何もデータが書き込まれていないので、ＥＥＰＲＯＭ２９のデータとメモリ２４に記憶された固定データとは一致せず、ディスエーブル信号はＨレベルとなっている。

【００４１】このため、上記した特定データ以外のデータであれば、ＥＥＰＲＯＭ２９に対して、外部からのデータの書き込み及び読み出しが可能となり、ＥＥＰＲＯＭ２９のテストも容易に行なうことができる。

【００４２】なお、図３に示した構成において、ＥＥＰＲＯＭ２９へのデータ書き込みに当たっては、同一データを繰り返し書き込む必要があるメモリもあり、この場合には、データの書き込みが完了するまでの期間中、フリップフロップ回路２６の出力をＨレベルに保持しておく必要があるが、その保持手段についての説明は省略する。

【００４３】図４は、上記したディスエーブル信号を発生するためのさらに他の例を示している。すなわち、セキュリティ回路２１には、ワンタイムＲＯＭ２２やＥＥＰＲＯＭ２９に代えて、レジスタ３２が設置されている。このレジスタ３２は、そのデータ入力端が読み出しデータＲＤＡＴＡの伝送ラインに接続され、そのデータ出力端がＥＸオア回路２３の一方の入力端に接続されている。また、このレジスタ３２のクロック入力端には、初期化回路２０から出力されるストローブ信号が供給されている。

【００４４】また、セキュリティ回路２１には、ロジック回路３３が設置されている。このロジック回路３３は、ホストＩ／Ｆ回路１３から出力される書き込みイネーブル信号ＷＥ，読み出しイネーブル信号ＲＥ，第１乃至第３のチップセレクト信号ＣＳ１～ＣＳ３と、フリップフロップ回路２６から出力されるディスエーブル信号と、初期化回路２０から出力される初期化パルスとに基づいて、前記ＥＥＰＲＯＭ１７に対する、チップセレクト信号ＣＳ，書き込みイネーブル信号ＷＥ及び読み出しイネーブル信号ＲＥを生成している。

【００４５】なお、このＥＥＰＲＯＭ１７は、その書き込みデータ入力端が書き込みデータＷＤＡＴＡの伝送ラインに接続され、その読み出しデータ出力端が読み出しデータＲＤＡＴＡの伝送ラインに接続されている。

【００４６】さらに、セキュリティ回路２１は、ＥＥＰＲＯＭ１７の特定のアドレスＡ１を指定するためのアドレスデータが書き込まれたメモリ３４を有しており、このメモリ３４に書き込まれたアドレスデータと、ホストＩ／Ｆ回路１３から出力される下位アドレスデータとが、初期化パルスで制御されるスイッチ３５によって選択的にＥＥＰＲＯＭ１７に導かれるようになっている。

【００４７】ここで、上記ロジック回路３３では、ＣＳ出力＝ＣＳ１＋ＣＳ２＋ＣＳ３＋初期化パルスのバー、ＷＥ出力＝（ＣＳ１＋ＣＳ２＊ディスエーブル信号＋ＣＳ３＊ディスエーブル信号）＊入力ＷＥ、ＲＥ出力＝（ＣＳ１＋ＣＳ２＋ＣＳ３＊ディスエーブル信号）＊入力ＲＥ＋（初期化パルスのバー）なる演算を行なうことにより、チップセレクト信号ＣＳ，書き込みイネーブル信号ＷＥ及び読み出しイネーブル信号ＲＥをそれぞれ生成している。

【００４８】図４に示す構成において、製造直後のテスト時に初期化回路２０に初期化要求信号ＩＮＩＴを供給すると、初期化回路２０は、Ｌレベルの初期化パルスを発生する。すると、スイッチ３５は、メモリ３４側に切り替わり、メモリ３４に記憶されているアドレスデータがＥＥＰＲＯＭ１７に供給される。

【００４９】また、この時点では、ホストＩ／Ｆ回路１３から出力される書き込みイネーブル信号ＷＥと読み出しイネーブル信号は共にＬレベルで、チップセレクト信号ＣＳ１～ＣＳ３は不定であり、フリップフロップ回路２６から出力されるディスエーブル信号はＨレベルとなっているが、初期化パルスがＬレベルであるために、ロジック回路３３からは、Ｈレベルのチップセレクト信号，Ｌレベルの書き込みイネーブル信号，Ｈレベルの読み出しイネーブル信号が出力される。

【００５０】このため、ＥＥＰＲＯＭ１７は、アドレスＡ１に記憶されているデータ（現時点では何も書かれていない）の読み出し状態となり、読み出されたデータが読み出しデータＲＤＡＴＡの伝送ラインに出力されることになる。

【００５１】その後、初期化回路２０に対する初期化要求信号ＩＮＩＴの供給が停止されると、初期化回路２０からは、１クロック期間分Ｈレベルとなるストローブ信号が発生されるので、読み出しデータＲＤＡＴＡの伝送ラインに出力されていたデータが、レジスタ３２にラッチされる。そして、これよりさらに１クロック期間経過後、初期化パルスがＨレベルになるので、スイッチ３５が下位アドレスデータの伝送ライン側に切り替えられる。

【００５２】この場合、レジスタ３２にラッチされたデータは何も書かれていなかった値であるから、メモリ２４の固定データとは一致せず、フリップフロップ回路２６からはＨレベルのディスエーブル信号が出力される。すると、ロジック回路３３では、上式の演算が、ＣＳ出力＝ＣＳ１＋ＣＳ２＋ＣＳ３、ＷＥ出力＝（ＣＳ１＋ＣＳ２＋ＣＳ３）＊入力ＷＥ、ＲＥ出力＝（ＣＳ１＋ＣＳ２＋ＣＳ３）＊入力ＲＥとなる。つまり、ＥＥＰＲＯＭ１７の全アドレス領域が外部からアクセス可能になり、テストが容易に行なわれる状態となる。

【００５３】この状態で、ＥＥＰＲＯＭ１７のアドレスＡ１に、メモリ２４に記憶されている固定データと同じ値の特定データを書き込み、再度、初期化回路２０に対して初期化要求信号を供給して停止させる。すると、今度は、ＥＥＰＲＯＭ１７のアドレスＡ１に記憶されている特定データがレジスタ３２にラッチされることになり、その結果、フリップフロップ回路２６からはＬレベルのディスエーブル信号が出力されることになる。

【００５４】このとき、ロジック回路３３では、上式の演算が、ＣＳ出力＝ＣＳ１＋ＣＳ２＋ＣＳ３、ＷＥ出力＝ＣＳ１＊入力ＷＥ、ＲＥ出力＝（ＣＳ１＋ＣＳ２）＊入力ＲＥとなる。つまり、ＥＥＰＲＯＭ１７に対し、チップセレクト信号ＣＳ１で指定される領域について書き込み及び読み出しを可能とし、チップセレクト信号ＣＳ２で指定される領域について書き込み不可で読み出しを可能とし、チップセレクト信号ＣＳ３で指定される領域について書き込み及び読み出しを不可とするように制御している。

【００５５】図５（ａ）は、ＥＥＰＲＯＭ１７のアクセス領域を示している。図中上部がアドレス値の小さい領域であるとする。外部から指定されたアドレスに基づいて、ホストＩ／Ｆ回路１３で生成されたチップセレクト信号ＣＳ１で指定される領域では、外部からの読み出しと書き込みとが共に可能となっている。

【００５６】また、外部から指定されたアドレスに基づいて、ホストＩ／Ｆ回路１３で生成されたチップセレクト信号ＣＳ２で指定される領域では、外部からの読み出しのみが可能となっている。さらに、外部から指定されたアドレスに基づいて、ホストＩ／Ｆ回路１３で生成されたチップセレクト信号ＣＳ３で指定される領域では、外部からの読み出しと書き込みとが共に不可となっている。

【００５７】そして、前記メモリ３４に書き込まれているアドレスＡ１は、チップセレクト信号ＣＳ３で指定される領域のアドレスとなっている。このため、チップセレクト信号ＣＳ３で指定される領域に秘匿データを書き込み、アドレスＡ１に固定データと同じ特定データを書き込んで、初期化することにより、秘匿データを外部からアクセス不可能にすることができる。

【００５８】このようなＥＥＰＲＯＭ１７のアクセス不能領域には、秘密を要する鍵データや暗号の非公開パラメータ、あるいは非公開の暗号処理アルゴリズムの実行プログラム等を書き込むことが有効である。また、ＥＥＰＲＯＭ１７の読み出し可能領域には、公開鍵データ等を書き込むことが有効である。

【００５９】暗号の非公開パラメータには、機器毎に値が異なるデータと、機器毎には同一値となるデータとがあり、後者のデータは、図１に示したＲＯＭ１５に書き込むことも可能であるが、ＥＥＰＲＯＭ１７のアクセス不能領域に書き込む方が望ましい。

【００６０】なぜならば、ＲＯＭ１５に書き込んだ場合、ＥＥＰＲＯＭ１７のアドレスＡ１に書き込んだ特定データが、何らかの原因で固定データと異なる値に変化して記憶されてしまうと、ＲＯＭ１５が外部からアクセス可能となって秘匿データが読み出されることになる。

【００６１】これに対し、ＥＥＰＲＯＭ１７のアクセス不能領域に書き込むと、製造検査が可能となるだけでなく、ＥＥＰＲＯＭ１７のアクセス不能領域に書き込まれたデータが何らかの原因で変化する場合には、同一領域に書き込まれた他の非公開データも同じように変化していると考えられるので、元の正規の非公開データが読み出されることは防止することができる。

【００６２】図５（ｂ）は、デジタルＬＳＩチップ１０内のＲＡＭ１６のアクセス領域を示している。このＲＡＭ１６に対しても、ＥＥＰＲＯＭ１７の場合と同様に、チップセレクト信号ＣＳｉで指定される外部からの読み出し書き込み可能領域と、チップセレクト信号ＣＳｉ＋１で指定される外部からの読み出しのみ可能領域と、チップセレクト信号ＣＳｉ＋２で指定される外部からのアクセス不可領域とを設定することができる。

【００６３】そして、例えば、このＲＡＭ１６の読み出し書き込み可能領域は、外部とのデータ通信領域として使用され、読み出しのみ可能領域は、内部状態を示すフラグ等の記憶領域として使用され、アクセス不能領域は、暗号処理時における中間データ等の非公開データを処理するために使用される。

11

【００６４】図６は、スクランブル処理における、そのテストと秘匿データの保護について説明している。すなわち、スクランブル回路１２は、入力データにスクランブル処理を施すシャッフル回路１２ａと、ホストＩ／Ｆ回路１３やコントロール回路１４からのアドレスをデコードするアドレスデコーダ１２ｂと、スクランブルキーを書き込むレジスタ１２ｃと、スクランブルのモードを決めるコントロールレジスタ１２ｄと、スクランブル回路１２の状態や入力データの状態を示す状態レジスタ１２ｅとを含んでいる。

【００６５】また、コントロール回路１４は、ゼネラルレジスタ１４ａと、命令レジスタ１４ｂと、アドレス発生器１４ｃとを含んでいる。さらに、暗号鍵解凍のための特殊演算器であるＡＬＵ１８は、入力レジスタ１８ａと、出力レジスタ１８ｂと、演算部１８ｃとを含んでいる。

【００６６】外部から、コントロール回路１４の命令レジスタ１４ｂに命令が書き込まれると、コントロール回路１４は、その命令に対応して、デジタルＬＳＩチップ１０の各回路を制御する。例えばスクランブルキーの解凍であるとすると、外部からＲＡＭ１６に暗号鍵データが書き込まれた後、その鍵の解凍命令が命令レジスタ１４ｂに書き込まれる。

【００６７】コントロール回路１４は、ＲＡＭ１６の暗号鍵データをＡＬＵ１８の入力レジスタ１８ａに書き込む。すると、ＡＬＵ１８の演算結果が、出力レジスタ１８ｂに現れる。コントロール回路１４は、出力レジスタ１８ｂのデータをゼネラルレジスタ１４ａに読み込み、スクランブル回路１２のレジスタ１２ｃに書き込むという一連のプログラムを実行する。外部からの命令実行が終了すると、コントロール回路１４は、その内部のステータスフラグを立て、あるいは割り込みを発生させて外部に通知する。

【００６８】デジタルＬＳＩチップ１０の製造検査時は、テストモードデータをテスト回路１９に与えて、各回路部分毎にテストができるようにする。例えばスクランブル回路１２をテストする場合には、ホストＩ／Ｆ回路１３を介してスクランブル回路１２の全てのレジスタが外部からアクセスできるように、内部接続が制御される。

【００６９】その後、仮のスクランブルキーをレジスタ１２ｃに書き込み、仮の規定データを入力データとしてシャッフル回路１２ａに供給する。そして、所定の期待値データが出力データとして得られるか否かを判別する。もし、スクランブル回路１２の一部が不良であった場合には、出力データが期待値と異なるので不良品であると判断することができる。ＡＬＵ１８についても同様な手法でテストすることができる。

【００７０】ここで、スクランブル回路１２のレジスタ１２ｃ，コントロール回路１４のゼネラルレジスタ１４ａ及びＡＬＵ１８の出力レジスタ１８ｂには、秘匿すべきデータがそれぞれラッチされているため、これらレジスタ１２ｃ，１４ａ，１８ｂの内容を外部からアクセスできないようにすることが、肝要なことになる。

12

【００７１】上記したセキュリティ回路２１によって、ディスエーブル信号がＨレベルのとき、内部の回路を自由に外部からアクセス可能とし、ディスエーブル信号がＬレベルのとき、上記レジスタ１２ｃ，１４ａ，１８ｂの内容を外部からアクセスできないように設定することで、テストを容易に行なうことができ、しかも秘匿データを確実に保護することができるようになる。なお、この発明は上記した実施の形態に限定されるものではなく、この外その要旨を逸脱しない範囲で種々変形して実施することができる。

【００７２】

【発明の効果】以上詳述したようにこの発明によれば、秘匿データに対しては外部からのアクセスを確実に阻止することができ、テスト時には信頼性の高い検査を容易に行ない得るようにした極めて良好なデジタル集積回路を提供することができる。

【図面の簡単な説明】

【図１】この発明に係るデジタル集積回路の実施の形態を示すブロック構成図。

【図２】同実施の形態における要部の一例を示すブロック構成図。

【図３】同実施の形態における要部の他の例を示すブロック構成図。

【図４】同実施の形態における要部のさらに他の例を示すブロック構成図。

【図５】同実施の形態におけるメモリのアクセス領域を説明するために示す図。

【図６】同実施の形態におけるスクランブル動作を説明するために示す図。

【図７】同実施の形態におけるデジタルＬＳＩチップを示す外観図。

【符号の説明】

１０…デジタルＬＳＩチップ、
１１…半導体基板、
１２…スクランブル回路、
１３…ホストＩ／Ｆ回路、
１４…コントロール回路、
１５…ＲＯＭ、
１６…ＲＡＭ、
１７…ＥＥＰＲＯＭ、
１８…ＡＬＵ、
１９…テスト回路、
２０…初期化回路、
２１…セキュリティ回路、
２２…ワンタイムＲＯＭ、
２３…ＥＸオア回路、

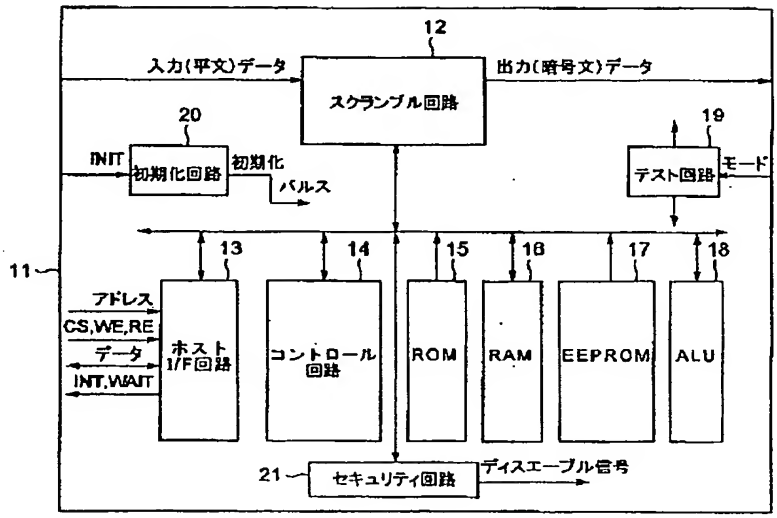
13

２４…メモリ、
２５…オア回路、
２６…フリップフロップ回路、
２７…アンド回路、
２８…アドレスデコーダ、
２９…ＥＥＰＲＯＭ、

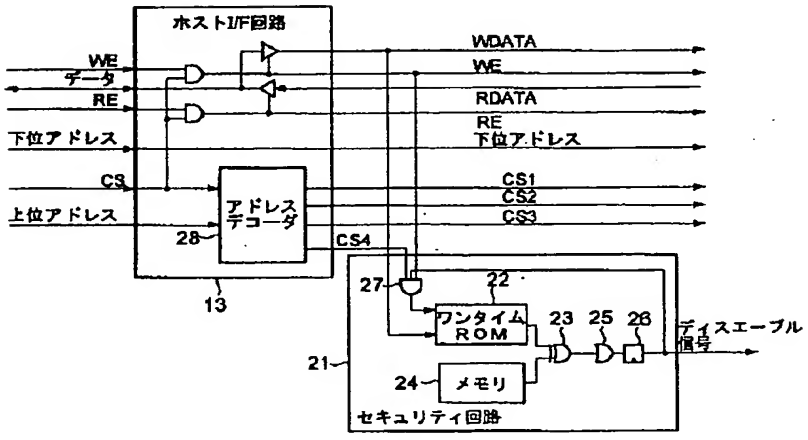
14

３０…３ステートバッファ、
３１…アンド回路、
３２…レジスタ、
３３…ロジック回路、
３４…メモリ、
３５…スイッチ。

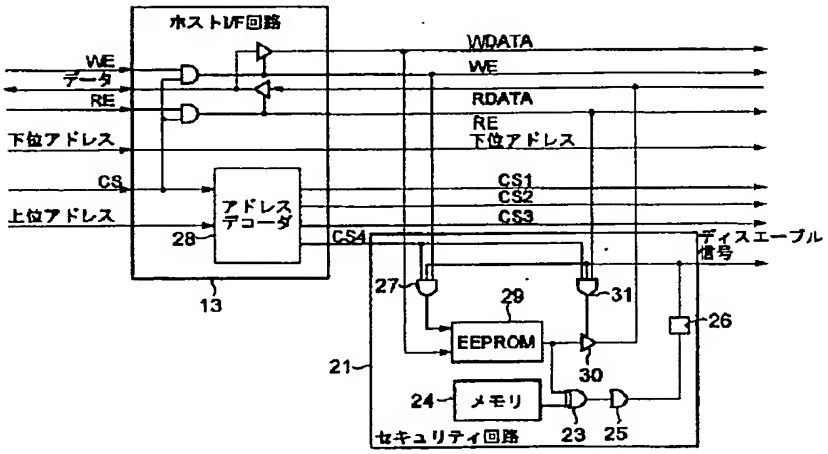
【図１】



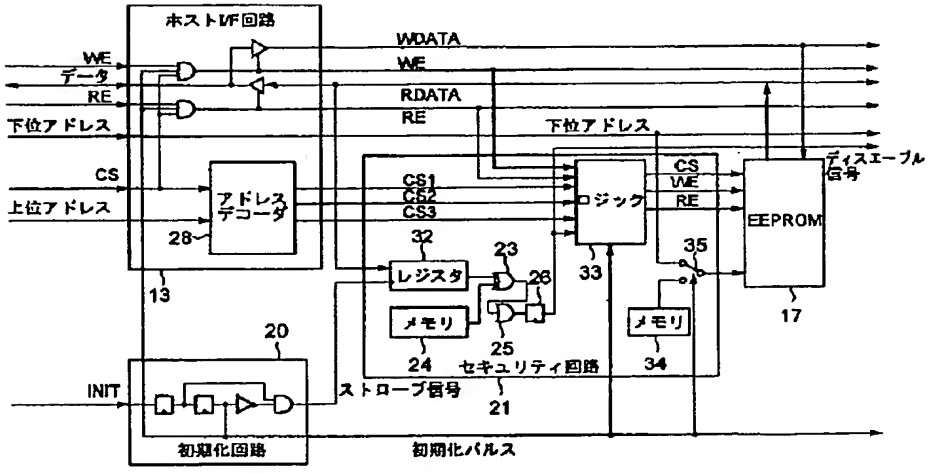
【図２】



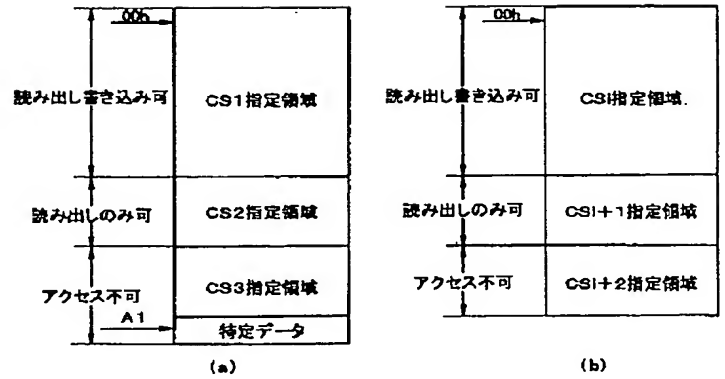
【図３】


ホストI/F回路
WE
データ
RE
下位アドレス
CS
上位アドレス
アドレス
デコーダ
28
13
WDATA
WE
RDATA
RE
下位アドレス
CS1
CS2
CS3
CS4
ディスエーブル
信号
27
29
31
EEPROM
26
30
21
24
メモリ
23
25
セキュリティ回路

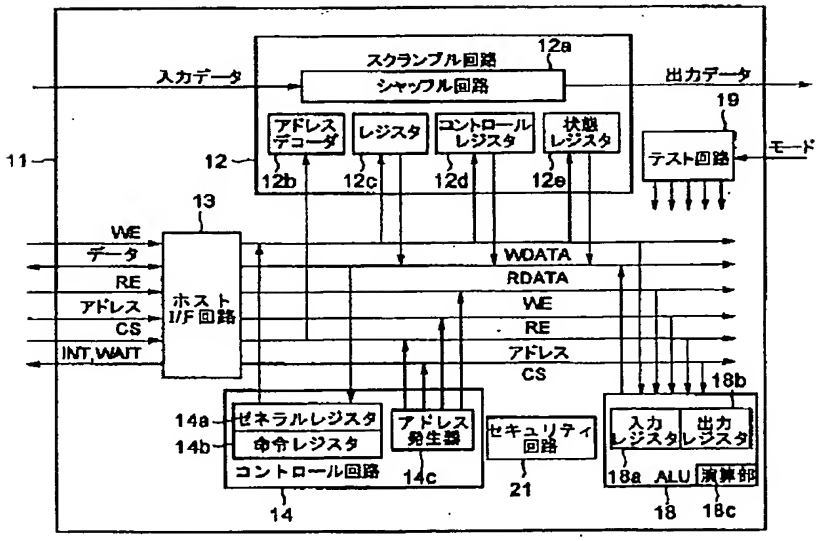
【図４】


ホストI/F回路
WE
データ
RE
下位アドレス
CS
上位アドレス
アドレス
デコーダ
28
13
WDATA
WE
RDATA
RE
下位アドレス
CS1
CS2
CS3
ロジック
CS
WE
RE
ディスエーブル
信号
EEPROM
17
32
レジスタ
23
26
33
35
メモリ
24
25
セキュリティ回路
メモリ
34
20
INIT
ストローブ信号
21
初期化回路
初期化パルス

【図５】


00h
読み出し書き込み可
CS1指定領域
読み出しのみ可
CS2指定領域
アクセス不可
CS3指定領域
A1
特定データ
(a)
00h
読み出し書き込み可
CSI指定領域
読み出しのみ可
CSI+1指定領域
アクセス不可
CSI+2指定領域
(b)

【図６】


入力データ
スクランブル回路
シャッフル回路
12a
出力データ
19
アドレスデコーダ
レジスタ
コントロールレジスタ
状態レジスタ
テスト回路
モード
11
12
12b
12c
12d
12e
13
WE
データ
RE
アドレス
CS
INT,WAIT
ホストI/F回路
WDATA
RDATA
WE
RE
アドレス
CS
18b
14a
14b
ゼネラルレジスタ
命令レジスタ
コントロール回路
アドレス発生器
14c
セキュリティ回路
21
入力レジスタ
出力レジスタ
18a
ALU
演算部
14
18
18c

【図７】